REMARKS

Of the originally filed claims 1-36, Applicant cancelled claims 31-36 without prejudice. Accordingly, claims 1-30 are currently pending. In the May 27, 2008 Office Action, the Examiner finally rejected claims 1-36 under 35 U.S.C. 102(b) as anticipated by U.S. Patent No. 6,134,550 to Van Oorschot et al. ("Oorschot"). Applicant respectfully traverses the rejection for the reasons set forth hereinbelow.

A. Claims 1-30 Are Not Anticipated by Van Oorschot

1. The "Transitive Closure Computation" Requirement Variously Recited In Claims 1-9, 24, 27, and 30 Is Not Anticipated by Van Oorschot

In response to the Examiner's original rejection of claims 1-9 as being anticipated by Van Oorschot, Applicant explained that Van Oorschot's disclosed system (for employing trusted paths to determine the validity of a certificate) does not anticipate the present invention's scheme for computing digital certificate trust paths by, *inter alia*, "performing a transitive closure computation on the adjacency matrix to generate a set of inter-CA trust path indicators that represent whether a trust path exists between a pair of certificate authorities." *See, e.g.*, claims 1, 24, 27, and 30. In response, the Examiner makes the wholly unsupported assertion that "the examiner disagrees. Oorschot reference discloses computing shortest path of all certificate authority in transitive adjacency matrix. (Oorschot: column 4, lines 64-67 and Figures 7a and 7b)." *See*, Final Office Action, p. 6. In reply, Applicant respectfully submits as a preliminary matter that the term "transitive adjacency matrix" is simply not an intelligible or understood term. But more importantly, the Examiner has provided no explanation of where exactly Van Oorschot discloses "performing a transitive closure computation" as claimed. While the Examiner has cited to Van Oorschot, col. 4, lines 52-57 to meet this requirement (Final Office Action, p. 2), there is simply no reference to any computation of the transitive closure in the cited passage, as readily seen from the cited passage quoted below:

> For example, where a high degree of compilation is performed, the certificate chain data may be a list of all certification authorities in a shortest trusted path starting with a subscriber's own CA and ending with the target CA that issued the certificate of the subscriber that sent a digitally signed message.

See, Van Oorschot, col. 4, lines 52-57. As best Applicant can tell, it appears that the Examiner may be confusing the "all-pairs-shortest-paths" computation with the

"transitive closure" computation. However, as seen in claim 1's separate recitation of the "transitive closure" and "all-pairs-shortest-path" computations, Applicant has distinctly claimed and described the "transitive closure" requirement which immediate determines whether a trust path exists between two certificate authorities before the actual path is determined:

> [0070] The **transitive closure** is then computed over the adjacency matrix (step 406). The **transitive closure** represents whether there is a path, i.e. set of edges, through the directed graph for any two nodes in the directed graph. Hence, the **transitive closure** can also be represented with a matrix with each cell reflecting whether or not there is a path between the entities that correspond to the row and the column for the cell.
>
> [0071] Several algorithms exist for computing the **transitive closure** matrix from an adjacency matrix; "Warshall's algorithm" is frequently used for this type of computation, which is also known as solving the reachability problem for a set of nodes in a graph.
>
> [0072] The present invention recognizes that a **transitive closure** computation can be applied to a trust web. The output of a **transitive closure** computation represents whether or not an established trust path exists between two certificate authorities that are involved in a certificate validation process; this output information may be termed "inter-CA trust path indicator information" as it quickly indicates whether or not a trust path exists between two certificate authorities. The result of the **transitive closure** computation is then stored in an appropriate format (step 408), e.g., a simple file containing the matrix, one or more database records, or some other format.
>
> [0073] <u>An "all pairs shortest paths" computation is then performed on the adjacency matrix (step 410)</u>. The shortest paths that are discovered during the "all pairs shortest paths" computation are then stored in an appropriate format (step 412), e.g., a simple file containing a set of paths, a set of files containing a vector representing a path, a set of linked list data structures, a set of one or more database records, or some other format. The "all pairs shortest paths" computation is described in more detail below.
>
> [0074] With reference now to FIGS. 5A-5B, the **transitive closure** computation and the "all pairs shortest paths" computation are depicted using an adjacency matrix that is used as input to the computations and the resulting matrices that are output from the computations.
>
> [0075] In one embodiment of the present invention, an adjacency matrix might represent only the existence of relations between nodes in a directed graph. In other words, a simple adjacency matrix might have cells in which a value of "0" in a cell represents the non-existence of a relation between the corresponding

> nodes for the cell and a value of "1" represents the existence of a relation. In the present invention, the cells along the diagonals of this type of adjacency matrix are filled with zeroes because a trust relation between a certificate authority and itself is not represented, although in the realm of digital certificates, a certificate authority can be viewed as "self-certifying".
>
> [0076] Referring to FIG. 5A, adjacency matrix 502 is depicted for the set of certificate authorities that are shown in FIG. 3B. Using this adjacency matrix, the **transitive closure** computation produces an output matrix in which each cell reflects whether or not there is a path between the entities that correspond to the row and the column for the cell. With respect to the present invention, output matrix 504 from the **transitive closure** computation represents a set of inter-CA trust path indicators that reflect whether or not there is a path between the corresponding certificate authorities.

See, Application, paragraphs 70-76 (emphasis added). As seen from the foregoing, the recited "transitive closure computation" is distinct from the "all-pairs-short-path" computation, and is used to determine, before the actual path is determined, whether there is a path through the directed graph for any two certificate authorities in the directed graph.

While Applicant has distinctly recited the claim requirement of "performing a transitive closure computation on the adjacency matrix to generate a set of inter-CA trust path indicators that represent whether a trust path exists between a pair of certificate authorities," the Final Office Action omits any explanation of how Van Oorschot anticipates this claim requirement since the cited passage (Van Oorschot, col. 4, lines 52-57) clearly makes no reference to such a "transitive closure computation." Applicant respectfully submits that this omission amounts to a failure to articulate a *prima facie* anticipation showing that each and every element of the claimed invention, arranged as required by claims 1-9, 24, 27, and 30, are found in the Van Oorschot reference, either expressly or under the principles of inherency. *See generally*, In re King, 801 F.2d 1324, 1326, 231 USPQ 136, 138 (Fed. Cir. 1986); Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick, 730 F.2d 1452, 1458, 221 USPQ 481, 485 (Fed. Cir. 1984). Because of at least these differences between Van Oorschot and claims 1-9, 24, 27, and 30, Applicant requests reconsideration and withdrawal of the anticipation rejection of claims 1-9, 24, 27, and 30.

2. The Requirement That A Certificate Authority Send "A Trust Relation Update Message To A Central Trust Web Agent" Variously Recited In Claims 10-30 Is Not Anticipated by Van Oorschot

In response to the Examiner's original rejection of claims 10-30 as being anticipated by Van Oorschot, Applicant explained that Van Oorschot's disclosed system (for employing trusted paths to determine the validity of a certificate) does not anticipate the present invention's scheme for computing digital certificate trust paths by, *inter alia*, having a certificate authority send "a <u>trust relation update message</u> to a central trust web agent, wherein the central trust web agent processes trust relation information for a set of certificate authorities within a trust web." *See, e.g.*, claim 10. Applicant also explained that Vam Oorschot fails to disclose the requirement variously recited in claims 22-30 of a central trust web agent which uses a "trust relation update message" from a certificate authority to modify a set of trust relations for the set of certificate authorities within the trust web. *See, e.g.*, claim 22. In the <u>Final Office Action</u>, the Examiner states that Applicant's arguments "have been fully considered," but then entirely fails to acknowledge or respond to the noted deficiency regarding "trust relation update message," instead asserting that "applicant mainly argues that the prior art of record does not disclose 'adjacency matrix', 'transitive closure computation on the adjacency matrix', and 'an all-pairs-shortest-paths computation'." *See*, <u>Final Office Action</u>, p. 6. Obviously, this characterization of Applicant's arguments does not mention or address the "trust relation update message" requirement.

As seen from the foregoing, the Examiner has provided no explanation of where exactly Van Oorschot discloses using "a <u>trust relation update message</u>" from a certificate authority at a central trust web agent which "processes trust relation information for a set of certificate authorities within a trust web," as variously recited in claims 10-30. Likewise, the Examiner has provided no explanation of where exactly Van Oorschot discloses "<u>modifying a set of trust relations</u> for the set of certificate authorities within the trust web <u>based on an indicated request in the trust relation update message</u>," as variously recited in claims 22-30. While the Examiner has cited Van Oorschot's disclosure (col. 5, lines 53-61 and col. 7, line 62 to col. 8, line 13) that the certificate chain data 209 and database 208 can be "periodically updated" (<u>Final Office Action</u>, pp. 3-4), there is simply

no reference in Van Oorschot of having a certificate authority send a "trust relation update message" to a central trust web agent, much less using the received "trust relation update message" to modify the set of trust relations at the central trust web agent as readily shown by the cited Van Oorschot passages quoted below:

> The certificate chain data 209 is compiled from certification authority trust data. Certification authority trust data may include for example, cross-certification data, revocation data and/or other data stored in a distributed directory (e.g., X.500 directories or LDAP-compliant repositories). The certificate chain data 209 is prepared once, and <u>periodically updated</u> as needed, for more than one subscriber and may be repeatedly used each time validation needs to occur.
>
> * * *
>
> <u>The certificate chain database 208 may be periodically updated</u>, for example <u>by the certificate chain data generator 400 periodically polling the distributed directory 302 or other sources of certificate data to determine whether updates in the certificate trust data has occurred</u> (additional certificates, revocation of certificates etc.) and recompiling the necessary database entries. For example, if a certification authority (CA) is added to the community of interest, the certificate chain data generator 400 obtains the new information from the directory 302 and adds any links based on the certification authority trust data associated with that new certificate issuing unit to incorporate the trust relationship as certificate chain data 209 in the certificate chain data database 208. Therefore where a database 302 includes certificates indicating cross-certification among certificate issuing units, the certificate chain data generator 400 uses the cross-certification information to note a trust path between the corresponding certificate issuing units.

Van Oorschot, col. 5, lines 53-61 and col. 7, line 62 to col. 8, line 13 (emphasis added). Indeed, Van Oorschot discloses a variety of techniques for updating the certificate chain database 208 (including periodically polling the distributed directory or other sources of certificate data), but conspicuously fails to disclose using trust relation update messages from the certificate authorities. In contrast, Applicant has distinctly claimed and described the role of the "trust relation update message" in "modifying a set of trust relations for the certificate authorities":

> [0095] T<u>he certificate authority then sends a trust relation update message to the central trust web agent (step 824)</u>; in a cross-certification operation, each certificate authority would be responsible for sending such a message to the central trust web agent. In response from the central trust web agent at some later point in time, the certificate authority would receive updated adjacency information, updated inter-CA trust path indicators (updated transitive closure information), and an updated set of shortest trust paths for the trust web (step 826). The certificate authority then stores this information for later use in a

certificate validation procedure (step 828), and the process is complete. In this manner, the central trust web agent assumes the responsibility for performing transitive closure computations and "all pairs shortest paths" computations for the trust web.

[0096] It should be noted that a certificate authority could receive updated information from the central trust web agent in response to an update from another certificate authority, thereby causing it to perform steps 826 and 828 without performing steps 822 and 824. This scenario could occur because, even though the certificate authority that receives this information does not have a direct trust relation with the certificate authority that caused the update, the receiving certificate authority could have a trust path with a certificate authority that established a new trust relation, which thereby affects the trust paths of the receiving certificate authority. Most certificate authorities should not be affected by a new trust relation, i.e. the effect should be localized, but it is possible that the effect could propagate throughout the trust web. This process is independent of any particular protocol that is used by the certificate authorities for establishing a new trust relation. In addition, this process is independent of any particular protocol or message format that is used to communicate information between the certificate authorities and the central trust web agent.

[0097] With reference to FIG. 8C, a flowchart depicts a process by which a central trust web agent generates and disseminates trust web information to certificate authorities within a trust web. The process begins when the trust web agent receives a trust relation update message from a certificate authority (step 832), and the trust relation within the receive message is added or deleted from the current set of trust relations that is maintained by the central trust web agent (step 834). The trust web agent then performs the transitive closure computation (step 836) and also the "all pairs shortest paths" computation (step 838), after which it can store the information for later use. By comparing the newly generated transitive closure information and shortest path information with the previously generated information, the central trust web agent can determine which certificate authorities have been affected by the most recent trust relation update. Hence, the central trust web agent can communicate the appropriate updated information to the affected certificate authorities (step 840), thereby completing the process from the perspective of the central trust web agent.

See, Application, paragraphs 95-97 (emphasis added).

While Applicant has distinctly recited the requirement of a "trust relation update message" that is sent to or received by a central trust web agent which "processes trust relation information for a set of certificate authorities within a trust web" in claims 10-30, the Final Office Action omits any explanation of how Van Oorschot anticipates this claim requirement. Nor does the Final Office Action explain how Van Oorschot discloses the requirement of "modifying a set of trust relations for the set of certificate authorities

within the trust web <u>based on an indicated request in the trust relation update message</u>" recited in claims 24-30. Accordingly, Applicant respectfully submits that this omission amounts to a failure to articulate a *prima facie* anticipation showing that each and every element of the claimed invention, arranged as required by claims 10-30, are found in the Van Oorschot reference, either expressly or under the principles of inherency. *See generally*, <u>In re King</u>, 801 F.2d 1324, 1326, 231 USPQ 136, 138 (Fed. Cir. 1986); <u>Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick</u>, 730 F.2d 1452, 1458, 221 USPQ 481, 485 (Fed. Cir. 1984). Because of at least these differences between Van Oorschot and the claims, Applicant requests reconsideration and withdrawal of the anticipation rejection of claims 10-30.

CONCLUSION

In view of the remarks set forth herein, Applicant respectfully submits that all pending claims are in condition for allowance and request that a Notice of Allowance be issued. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the examiner is requested to telephone the undersigned at 512-338-9100.

CERTIFICATE OF TRANSMISSION

I hereby certify that on July 28, 2008 this correspondence is being transmitted via the U.S. Patent & Trademark Office's electronic filing system.

/Michael Rocco Cannatti/

Respectfully submitted,

/Michael Rocco Cannatti/

Michael Rocco Cannatti
Attorney for Applicant(s)
Reg. No. 34,791